UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

FREDY GIRON, individually and on behalf of others similarly situated, **Plaintiff,** **vs.** **VTECH ELECTRONICS NORTH AMERICA, L.L.C.,** **Defendant.**	**CASE NO. 1:15-cv-11885** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

I. INTRODUCTION

Plaintiff Fredy Giron ("Plaintiff"), individually and on behalf of all others similarly situated, files this Class Action Complaint against VTech Electronics North America, L.L.C. ("Defendant" or "VTech"), and alleges as follows based on personal knowledge, the investigation of his counsel, and information and belief.

II. NATURE OF THE ACTION

1. In what has been described as a "parent's nightmare of epic proportions," more than ten million parents, legal guardians, and minor children ("VTech Customers") became the victims of a massive data breach, when their personally identifiable information ("PII") was accessed and downloaded from VTech's servers by a hacker on or about November 14, 2015 (the "Data Breach"). The Data Breach is the fourth largest consumer data breach to date, and is the largest known data breach involving the personal information of minor children.

2. The Data Breach resulted in the disclosure of registered adult VTech Customers' sensitive PII, including their names, addresses, email addresses, IP addresses, passwords, and secret questions and answers. It also resulted in the disclosure of associated minor children's names, genders, and birthdays. Moreover, the PII of those minor children is linked with that of the registered adult VTech Customers, such that anyone with access to the hacked data not only knows the names, genders, and ages of the affected children, but may also learn their home addresses. In addition, the Data Breach also exposed tens of thousands of photographs of children and their parents or other trusted adults—more than 190 GB of photographs—as well as audio files and a year's worth of chat logs between minor children and their parents or other trusted adults. Most if not all of these photographs, recordings, and logs can be traced back to specific usernames, so that anyone in possession of the hacked data can identify who is in a given photograph, recording, or chat log.

3. The Data Breach puts registered adult VTech Customers whose sensitive PII was compromised at increased risk of identity theft for years, and potentially for a lifetime, because names, legal relationships, facial characteristics, vocal characteristics, and truthful answers to many standard security questions are difficult to change.

4. Even worse, the information compromised in the Data Breach is linked to additional extensive information about the minor children, including their age, gender, and facial and vocal characteristics, which places these VTech Customers at increased risk of exposure to criminal acts of child predators. As one security expert observed, "people who prey on children—now have the ability to get basic information about them—where they live, what they look like," cautioning that "this lapse of security" would potentially allow such predators to gain the trust of children whose information was compromised. Another security expert has expressed

similar concerns: "When [the data] includes their parents as well—along with their home address—and you can link the two and emphatically say 'Here is 9 year old Mary, I know where she lives and I have other personally identifiable information about her parents (including their password and security question),' I start to run out of superlatives to even describe how bad that is."

5. Cybercriminals were able to perpetrate a breach of this depth and scope because VTech failed to maintain reasonable and adequate security measures to protect the information of VTech Customers using VTech's services from access and disclosure. VTech has obligations, by statute and otherwise, to protect its customers' PII from unauthorized access, yet failed, despite numerous opportunities, to prevent, detect, end, or limit the scope of the breach. Among other things, VTech failed to: (1) implement security measures designed to prevent this attack; (2) employ security protocols to detect the breach and removal of more than 190 GB of data from its computer networks; and (3) maintain basic security measures such as encryption, which would have ensured that, in the event data were accessed or stolen, it would be unreadable and thus cause less damage to VTech Customers and their families. Thus, VTech's conduct is a direct cause of the ongoing harm customers and their families are currently suffering and will continue to experience for years, and potentially for a lifetime.

6. Following the breach, VTech failed to detect the unauthorized access of data from its servers, until it was contacted by Motherboard, a news organization investigating the story. Even then, VTech failed to respond or notify its customers for several days after being notified by Motherboard. Ultimately, VTech responded to Motherboard on Thursday, November 26, confirming that "an unauthorized party accessed VTech customer data," and that VTech was "not aware of this unauthorized access until [Motherboard] alerted us." VTech then announced

the breach by press release on Friday, November 27, but failed to disclose the severity of the breach, including the number of records that were accessed or the fact that the PII of minor children was compromised. In this regard, VTech's delay left its customers in the dark about the scope of the breach, how they and their families were impacted, and what steps VTech is taking to remedy or mitigate the breach. Moreover, even though VTech has since provided additional information about the Data Breach, it continues to mislead its customers as to several key details about this breach. First, VTech declined to confirm that the hacker accessed tens of thousands of photographs of parents and children, despite the evidence to this effect. Second, VTech noted that any such pictures were encrypted, but did not add that this encryption is easy to break. Third, VTech indicated that chat logs were only stored on its servers for 30 days, when there is evidence that such logs were retained for a year.

7. Plaintiff is a VTech Customer who brings this proposed class action lawsuit on behalf of all VTech Customers in the United States whose PII has been compromised as a result of the Data Breach. Despite all best efforts of Plaintiff, VTech Customers, or anyone else, this most sensitive PII can never be made private again. Because the PII compromised in the Data Breach is difficult to change without significant time and/or expense, it is particularly valuable to cyber criminals and child predators who pay to use such information. As a result, Plaintiff and class members have already suffered from anxiety, stress and emotional distress, and have or will be required to spend time and/or money to remain vigilant for years, and potentially for the remainder of their lives, to thwart further unauthorized use of their sensitive PII by cyber criminals and child predators that seek to use it.

8. Plaintiff alleges that VTech failed to adequately safeguard the sensitive PII of VTech Customers using its services, in compliance with applicable law. Plaintiff seeks injunctive

relief requiring VTech to implement and maintain security practices to comply with regulations designed to prevent and remedy these types of breaches, as well as restitution, damages, and other relief.

III. JURISDICTION

9. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds $5 million, exclusive of interest and costs, and members of the proposed class are citizens of different states than Defendant VTech.

10. This Court has personal jurisdiction over VTech because VTech maintains its principal place of business in Arlington Heights, Illinois, is registered to conduct business in Illinois, and has sufficient minimum contacts with Illinois.

11. Venue is proper in this district under 28 U.S.C. § 1391(b) because VTech resides in this district, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this district.

IV. PARTIES

A. Plaintiff Fredy Giron

12. Plaintiff Fredy Giron is a resident of Texas who purchased a VTech Kidizoom Smartwatch DX ("VTech Device"), which is an electronic product aimed at children. In purchasing the VTech Device, Plaintiff paid a premium as compared to comparable devices for the advertised benefit of being able to download additional games and clock face designs from VTech's online service, Learning Lodge.

13. In order to make full use of the features of the VTech Device, Plaintiff Giron was required to download and install VTech's Learning Lodge software. Plaintiff Giron was also required to create an account with VTech in order to download content to the VTech Device through the Learning Lodge online service. In the process of creating an account with VTech,

Plaintiff Giron submitted his PII to VTech, including his name, email address, password, secret question and answer, home address, as well as his credit card number and billing information. Plaintiff Giron also submitted the PII of his minor child, for whom he purchased the VTech Device, including his child's name, gender, birthday, and photograph.

14. In providing his PII and that of his minor child to VTech, Plaintiff Giron expected that it would be reasonably safeguarded and protected against unauthorized access to maintain its confidentiality. Plaintiff Giron also expected that VTech would reasonably limit the amount of data and information that VTech captured and stored regarding him and his minor child.

15. Plaintiff Giron learned about the VTech data breach in December 2015.

16. Plaintiff Giron was not notified by VTech that his PII and that of his minor child was compromised in the Data Breach.

17. Based upon the information he has gathered about the Data Breach, Plaintiff Giron has a good faith basis to believe that his PII and that of his minor child was compromised in the Data Breach, causing current injury to Plaintiff Giron and his minor child and placing them at an increased risk of future injury from identity thieves and child predators.

18. Since learning of the Data Breach, Plaintiff Giron has suffered stress, anger, and anxiety because his PII and that of his minor child has been compromised in the Data Breach.

19. Plaintiff Giron has also been injured because the Learning Lodge service, for which he paid a premium, has been suspended and taken offline, and he can no longer access this service.

20. Plaintiff Giron is careful to protect the confidentiality of his PII as well as that of his minor child and other family members.

21. Plaintiff Giron has spent and continues to spend time and effort attempting to protect and safeguard himself, his minor child, and other family members against the potential consequences of the Data Breach, including investigating ways to protect against the risks the Data Breach has created.

22. If VTech had promptly notified Plaintiff Giron that his PII and that of his minor child had been compromised in the Data Breach, Plaintiff Giron would have been able to expedite the process of protecting himself, his minor child, and other family members against the risks the Data Breach has created.

23. Had Plaintiff Giron been aware of Defendant's excessive and unnecessary collection of PII, or its inadequate and negligent data security practices, he would not have purchased the VTech device, nor would he have downloaded, installed, and submitted his PII and that of his minor child to use the Learning Lodge service.

24. Going forward, Plaintiff Giron anticipates spending considerable time and money for the rest of his life to protect himself, his minor child, and other family members against the risks the Data Breach has created, including diligently monitoring his accounts and credit report for unauthorized use of his PII, as well as doing the same for his minor child and other family members.

B. Defendant VTech Electronics North America, L.L.C.

25. Defendant VTech Electronics North America, L.L.C. ("VTech") is a corporation organized under the laws of the State of Illinois, with its principal place of business in Arlington Heights, Illinois.

26. Defendant VTech's parent company, VTech Holdings Ltd., is a Bermuda corporation with its principal place of business in China.

V. FACTUAL ALLEGATIONS

A. VTech Encouraged VTech Customers To Share Their Sensitive PII With VTech

27. VTech is a company dedicated to making electronic products and delivering associated services to young children.

28. VTech represented to customers that its internet-capable VTech Devices incorporated parental controls to regulate the type of content children can access. The most prominent of these features involves the VTech Device's Web browser and other applications that require Internet connectivity. Parents and legal guardians can further edit settings and preferences for viewing websites within the browser itself, which allow parents to approve websites for children to view, specify time periods and maximum daily usage in which the Web browser will be available to the child, and monitor website viewing history.

29. Children cannot launch the Web browser or any Internet-dependent apps on a VTech Device until their parents or legal guardians register the VTech Device with VTech's Learning Lodge or Kid Connect online services. Learning Lodge allows users to download applications, electronic books, and games and tracks the child's learning achievements and games played. Kid Connect allows children to send texts and audio to parents and other connections approved by the parent or guardian using a smartphone application.

30. When registering for an account with VTech, VTech requires adult VTech Customers to supply PII, including their name, home address, email address, password, and secret question and answer. In addition, VTech requires additional PII to be supplied for minor children VTech Customers, including children's names, genders, and birthdays. Further, VTech links adult and child VTech accounts, so their PII is linked to additional PII, including their home addresses. Also, when registering to use VTech's online services, parents and children are

encouraged to take or upload photographs of themselves to use to identify themselves when using this text and voice service.

31. VTech further encouraged VTech Customers to share their sensitive PII through misrepresentations contained in its Privacy Policy. VTech's Privacy Policy for its www.vtechkids.com website, which was accessed on December 3, 2015, provides as follows.

> **5.1 Transmission and Storage of Your Information.** The security of your personal information is important to VTech, and VTech is committed to handling your information carefully. In most cases, if you submit your PII to VTech directly through the Web Services it will be transmitted encrypted to protect your privacy using HTTPS encryption technology. Any Registration Data submitted in conjunction with encrypted PII will also be transmitted encrypted. Further, VTech stores your PII and Registration Data in a database that is not accessible over the Internet.

32. As detailed below, VTech's Privacy Policy misrepresentations stand in marked contrast to what has been revealed about VTech's inadequate data security practices in the wake of the Data Breach.

33. For instance, security expert Troy Hunt reports that VTech has "no SSL anywhere" and "[a]ll communications are over unencrypted connections including when passwords, parent's details and sensitive information about kids is transmitted."

34. Further, the very fact of the Data Breach, in which PII and registration data was accessed through VTech's website, makes apparent the falsity of VTech's statement that it "stores [customers'] PII and Registration Data in a database that is not accessible over the Internet."

35. In addition to the PII VTech obtained when accounts were created to use Learning Lodge and Kid Connect, VTech also collected additional PII of VTech Customers using VTech Devices. This PII included photographs of parents, other trusted adults, and children; chat logs up to one year old; and audio recordings of conversations between parents, trusted adults, and

children. This additional PII also included IP addresses and download history, as well as the names of contacts for VTech Customers using the Kid Connect service.

36. Some of the PII VTech collected from its customers, including some photographs, chat logs, and audio recordings, does not serve any legitimate or necessary business purpose, and should not have been collected and stored by VTech on its servers. In this regard, VTech has failed to adequately explain why it was collecting and storing this information.

B. VTech Failed To Adequately Safeguard the PII of VTech Customers From Unauthorized Access

37. In collecting the sensitive and personal PII of VTech Customers, VTech had a legal obligation to safeguard this information so as to prevent it from being accessed by unauthorized users. However, even VTech has admitted that its customer "database was not as secure as it should have been."

38. VTech Customers purchased VTech Devices and signed up for VTech's online services with the reasonable expectation that VTech would provide reasonable and necessary data security to protect their confidential information. Similarly, VTech Customers used VTech Devices and services with the reasonable expectation that VTech would not collect or store information beyond that which was necessary for their use of these products and services. Had the VTech Customers known that their reasonable expectations would not be met as to the privacy and security of their confidential information, or as to the limitations on the data collected and stored by VTech, these customers would not have purchased the VTech Devices or signed up for VTech's online services.

39. Security experts who have evaluated VTech's security practices in the wake of the Data Breach have found a number of major flaws in VTech's security practices, which fall well below reasonable standards, and placed the PII of VTech Customers at unreasonable risk of

unauthorized access. In this regard, security expert Troy Hunt has written that VTech has shown a "total lack of care . . . in securing this data," in that it took him "no much more than a cursory review of publicly observable behaviors to identify serious shortcomings that not only appear as though they could be easily exploited, [but] evidently have been."

40. For instance, Hunt observed that VTech does not use SSL web encryption anywhere on its web pages. As a result, all data transmitted to or from VTech's web pages—including passwords—is unprotected in transit. Because of this, "you don't even need a data breach" for the PII of parents and children to be intercepted and accessed by an unauthorized individual.

41. Further, VTech's web pages were vulnerable to a SQL injection attack, which is "a simple and extremely common hacking technique in which hackers enter commands into website forms in order to make websites serve desirable data." This "ancient" technique is one that "even the teenager next door could probably pull off" and is "easy to defend against," but VTech failed to secure its databases against even such a simple attack.

42. Likewise, VTech's websites make "extensive use of Flash," which is "increasingly frowned upon in the security space" because of its "continuous stream of security vulnerabilities." For this and other reasons, Hunt views VTech's websites as being characterized by "systems from a bygone era," such that there is "the distinct sense VTech's assets were created a long time ago and then just... left there."

43. Not only did VTech fail to protect against unauthorized access to its database, VTech also failed to implement secondary protections that would have limited access to its data in the event of such unauthorized access. For example, VTech could have encrypted the PII of VTech Customers using its services, so that it would be difficult or impossible to unscramble and

use if it was accessed, but failed to do so. Although VTech did encrypt the passwords it stored, it did so using a very weak algorithm in a manner that is considered easy to break. On this subject, Troy Hunt wrote that "[t]he *vast* majority of these passwords would be cracked in next to no time," and that VTech's encryption represents "about the next to worst thing you do next to no cryptographic protection at all." The remainder of the PII stored by VTech was stored with no cryptographic protection whatsoever.

44. VTech also fails to adequately monitor its databases so as to identify when unauthorized access to its data is occurring or has occurred. For example, in the Data Breach at issue here, an unauthorized individual was able to download more than 190 GB of photographs and other data without VTech becoming aware of it. It was only after the unauthorized individual alerted a news organization, Motherboard, and that news organization contacted VTech, that VTech became aware of the Data Breach. In an email to Motherboard, a spokesperson for VTech wrote that "[w]e were not aware of this unauthorized access until you alerted us." As a result of VTech's failure to monitor the PII of VTech Customers that it collects, and particularly in light of VTech's other inadequate security measures, the Data Breach that is the subject of this litigation may be only one of many instances of unauthorized access to the PII collected and stored by VTech.

45. Even now, in the wake of the data breach, and "despite [VTech's] assurances that their system is now secure," Hunt writes that VTech "still [has] gaping holes that allow every kid to be matched with every parent." In this regard, "[t]he flaws are fundamental" and "there's no simple fix," such that Hunt has recommended that VTech's webpages be taken offline until their problems can be adequately addressed.

46. It would have been relatively easy for VTech to identify and correct the security deficiencies identified above. In this regard, security expert Mark Bower stated that such security risks "can be mitigated easily today," and that "vendors who truly value the security of their customer, and more importantly sensitive minor children's data, can get ahead of the attack and compliance challenges in one swoop by adopting modern data-centric security to secure the data in use, in motion and in transit—not just the increasingly translucent IT perimeter." Had VTech taken such steps and adopted such security, the Data Breach could have been prevented, the sensitive PII of VTech Customers might still be secure, and this litigation could have been avoided.

47. Indeed, in a misguided attempt to downplay the significance of the compromised PII of VTech Customers, VTech admitted that has taken additional security measures to ensure its ability to get paid:

> It is important to note that our customer database <u>does not</u> contain any credit card information and VTech does not process nor store any customer credit card data on the Learning Lodge Web site … To complete the payment or check-out process of any downloads made on the Learning Lodge Web site, our customers are directed to a *secure*, third-party payment gateway.

48. *Data Breach on VTech Learning Lodge*, VTech (Nov. 27, 2015) (underlining in original, italics added).

49. As noted by security expert Mark Bower, however: "Breach of children's data in itself has many serious risks, as you could imagine, and anyone collecting such data must take steps to protect it from advanced attacks as in [the VTech Data Breach]."

50. For this reason, VTech's security practices are subject to heightened regulation by the Federal Trade Commission through the Children's Online Privacy Protection Act of 1988, 15 U.S.C. 6501, *et seq.*("COPPA") and its associated regulations at 16 C.F.R. §312.1, *et seq.*, which

restricts "the collection, use, and/or disclosure of personal information from and about children on the Internet".

C. On Account Of VTech's Inadequate Security Measures, the PII of VTech Customers Was Accessed by Unauthorized Individuals

51. On or about November 14, 2015, "an unauthorized party accessed VTech customer data on [its] Learning Lodge app store customer database."

52. An individual has claimed responsibility for the Data Breach, and this hacker shared some of the data obtained from VTech with the news organization Motherboard. In turn, Motherboard shared this data with security expert Troy Hunt, who confirmed that the data appeared to have been obtained by an unauthorized individual.

53. The hacker was interviewed by Motherboard and revealed more information about the unauthorized access. In this regard, the hacker said that the database was accessed through a SQL injection hacking technique. In response, one security expert has stated that "[i]f that is the case then it really is unforgivable—it is such an old attack that any standard security testing should look for it." Further, the hacker indicated that "[a]ll the evidence suggested I wasn't the only person outside of VTech who could have got the data," adding that "someone with darker motives could easily get it."

54. The Data Breach resulted in the disclosure of adult VTech Customers' sensitive PII, including their names, addresses, email addresses, IP addresses, passwords, and secret questions and answers. It also resulted in the disclosure of minor children VTech Customers' names, genders, and birthdays. Moreover, the PII of children is linked with that an associated adult VTech Customer, such that anyone with access to the hacked data not only knows the names, genders, and ages of the affected children, but, in cases where the associated VTech Customer is the child's parent or legal guardian, also knows the child's home address and

information about the child's parent and/or legal guardian. In addition, the Data Breach also exposed tens of thousands of photographs of children and, in most cases, their parents or guardians—more than 190 GB of photographs—as well as audio files and a year's worth of chat logs between, for the most part, children and their parents. Most if not all of these photographs, recordings, and logs can be traced back to specific usernames, so that anyone in possession of the hacked data can identify who is in a given photograph, recording, or chat log.

55. Not only is the PII of adult and associated minor child VTech Customers linked together, but so too are the accounts of other users of the Kid Connect service who are listed as contacts. In this regard, the hacker stated that "I can get a random Kid Connect account, look through the [data] dump, link them to their circle of friends, and the parent who registered at Learning Lodge." Similarly, the hacker said that "I have the personal information of the parent and the profile pictures, emails, passwords, nicknames . . . of everyone in their Kid Connect contacts list."

56. The scope of the Data Breach is unprecedented. Not only is it the fourth largest consumer data breach to date, but it is the largest known data breach involving the personal information of children. In that the children registering for accounts with VTech are, on average, five years old at the time of registration, many of the children whose PII was compromised have not even entered kindergarten. As some commenters have noted, the Data Breach has compromised the PII of children "who don't even know what PII is."

D. VTech Failed To Identify, Respond To, Or Adequately Notify VTech Customers About the Data Breach

57. When the Data Breach occurred, VTech failed to identify that unauthorized access to its database had occurred, and consequently failed to notify affected individuals or respond in any way. It was only because the hacker reached out to the news organization Motherboard with

details about the Data Breach, and Motherboard provided these details to VTech, that VTech became aware that its data had been compromised. Even then, after VTech was alerted of the Data Breach by Motherboard on November 23, it took days for VTech to notify its customers.

58. On November 27, 2015, VTech issued a press release about the Data Breach. However, this press release failed to provide notice of the full extent of the Data Breach. To begin with, the press release indicated that the Data Breach was limited to the Learning Lodge app store, whereas it also extended to the Kid Connect service. Also, it failed to provide any information regarding the scope of the breach, which has since been revealed to include the PII of more than 10 million VTech Customers. Moreover, no mention was made of the fact that the PII of children was included in the Data Breach, nor of the fact that photographs, chat logs, and audio recordings were accessed.

59. On November 27, 2015, news organization Motherboard reported the Data Breach to the public in an article titled "One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids." This article included details as to how unauthorized access to the data occurred: "the hacker, who requested anonymity, told Motherboard that they gained access to the company's database using a technique known as SQL injection." On November 28, 2015, security expert Troy Hunt published a detailed blog post regarding his investigation of the Data Breach, titled "When Children Are Breached—Inside the Massive VTech Hack." In this article, Hunt confirmed that "a SQL injection attack . . . was the most likely attack vector," noting that, "[o]n seeing the haphazard way that internal database objects and queries are returned to the user, I've no doubt in my mind that SQL injection flaws would be rampant." Moreover, Hunt cautioned that, "despite [VTech's] assurances that their system is now secure, they still have

gaping holes," and recommended that VTech take its affected websites offline until they can be properly fixed.

60. On November 30, 2015, VTech issued an updated press release about the Data Breach. This press release suffered from the same deficiencies as the November 27 press release, failing to provide information regarding the scope of the breach, the contents of the data that was accessed, and the fact that the PII of children had been compromised. In this press release, VTech provided the additional information that it had "reached out to every account holder in the database, via email, to alert them of this data breach and the potential exposure of their account data." Further, VTech stated that "as an additional precautionary measure, we have suspended Learning Lodge" as well as a selection of its websites "for thorough security assessment and fortification."

61. Despite having been notified of the Data Breach on November 23, 2015, VTech waited until November 27 to notify VTech Customers that their sensitive PII had been compromised. Moreover, not only did VTech downplay the severity of the data breach, but it also failed to take their database offline until days after their initial notice. After publication of the Data Breach—including details about the security vulnerabilities that were exploited in making the attack—and before the database was taken offline, VTech's database was highly vulnerable to additional unauthorized access by hackers using the same methods employed in the November 14 Data Breach. As a result, it is possible if not likely that additional unauthorized access to the PII of VTech's customers and family members occurred during this time period.

62. On December 3, 2015, VTech issued an "Update on VTech Cyber Attack Incident," in which it announced that VTech has retained FireEye's Mandiant Incident Response services to assist it with responding to the Data Breach and strengthening the security of its

systems. Despite being aware that the unauthorized access likely occurred as a result of a simple SQL injection attack that would have been easy to defend against, VTech characterized the Data Breach as an "orchestrated and sophisticated attack on [its] network." Again, this press release suffered from the same deficiencies as the November 27 press release, failing to provide information regarding the scope of the breach, the contents of the data that was accessed, and the fact that the PII of children had been compromised.

63. VTech's repeated failures to inform VTech Customers that their sensitive PII was compromised in the Data Breach, as well as its subsequent attempts to downplay the risks posed to minor children VTech Customers whose PII was compromised, has caused them anxiety, stress and emotional distress and places them at increased risk of financial, physical, and/or emotional harm. As security expert Alan Woodward has cautioned, VTech should be "alerting the parents as soon as possible, with particular emphasis on how their children might be approached using this type of data." VTech's continuing failure to provide such a warning to parents, apparently in an attempt to downplay the significance of the Data Breach, increases the risk of harm to individuals whose PII was compromised in the Data Breach.

64. On December 3, 2015, VTech also updated its FAQ about Data Breach on VTech Learning Lodge, providing additional information about the Data Breach, including the following.

- That the Data Breach extended to VTech's Kid Connect servers as well as its Learning Lodge app store customer database;
- That approximately 4.9 million parent accounts and approximately 6.4 million children profiles were compromised, totaling more than 11 million people; and
- That approximately 1.2 million of the affected children profiles had Kid Connect enabled.

65. Despite providing this additional information, VTech is still misleading the public about the extent of the data breach. In response to the question "How could the hackers have hacked into your database so easily?" VTech asserted that the Data Breach was "a well-planned attack" conducted by "a skilled hacker," rather than admitting to the deficiencies in its security. Further, despite evidence that photographs of parents and children, chat logs, and audio files were compromised in the Data Breach, VTech writes that it "cannot confirm [this] at this stage" because "the investigation is on-going." Similarly, VTech asserts in this document that the passwords that were accessed were encrypted, despite its awareness that the encryption it used could be easily broken in most instances. Likewise, VTech asserts that photographs, chat logs, and related materials that might have been accessed in the Data Breach were encrypted, despite evidence that the hacker viewed and shared these materials. As a result of these misrepresentations, affected customers are likely to underestimate the extent and severity of the Data Breach, and will consequently be less likely to take steps to protect themselves against the harms, injuries, and damages that might result from the Data Breach.

E. The Data Breach Exposed Sensitive PII That Is Highly Valuable and Places Victims at Increased Risk of Identity Theft and Crime

66. The PII that was stolen in the Data Breach is highly valuable, and is estimated to be worth millions of dollars. Security expert Justin Harvey has said that each stolen account is worth between $1 and $4 in underground markets. Given that more than 11 million accounts were compromised in the Data Breach, the value of the data may therefore be estimated at between $11 million and $44 million.

67. An identity thief uses another's personal information, such as the person's name, address, birthday, and other information, without permission, to commit fraud or other crimes. They use this information to open new financial accounts and incur charges in another person's

name, take out loans in another person's name, and incur charges on existing accounts. They may also commit various types of crimes, from immigration fraud, obtaining a driver's license or identification card in the victim's name, using the victim's information to obtain government benefits, to filing a fraudulent tax return using the victim's information to obtain a refund. Identity thieves may also commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

68. There is a strong likelihood that VTech Customers are already or will become victims of identity fraud given the breadth of information about them that was accessed in the Data Breach. Javelin Strategy & Research reported in its 2014 Identity Fraud Study that "[d]ata breaches are the greatest risk factor for identity fraud." In fact, "[i]n 2013, one in three consumers who received notification of a data breach became a victim of fraud." Javelin also found increased instances of fraud other than credit card fraud, including "compromised lines of credit, internet accounts (e.g., eBay, Amazon), and email payment accounts such as PayPal." As a result of the Data Breach, there is a significant risk of fraud relating to online accounts, because the data compromised in the breach included passwords as well as secret questions and answers, which could be used to access or reset the passwords of other online accounts linked to email addresses contained in VTech's database.

69. The sensitive PII of minor children VTech Customers compromised in the Data Breach is particularly valuable to identity thieves. In contrast to adults, where identity theft and credit fraud is often detected by victims or financial institutions, the children whose PII was compromised might not apply for credit or set up a bank account for many years. As a result, by the time these children apply for credit, "they may discover that their credit score has been destroyed long ago by identity thieves." In this regard, security expert Jessy Irwin has cautioned

that the identities of these children are "blank slates that no one checks on until college years." Similarly, security expert Avner Levin stated that "[k]ids could be impacted with bad credit ratings and big difficulties down the line," because "criminals can take that basic biographical information [that was compromised in the Data Breach] and pretend they are the child to commit identity theft." The fact that the birthdays of children were compromised in the Data Breach puts them at increased risk of identity theft, because "a full name, date of birth and mailing address are often sufficient to open a fraudulent account."

70. Not only does the Data Breach put VTech Customers at increased risk of identity theft and fraud, but the extensive information revealed about the children whose PII was exposed put them at increased risk of exposure to criminal acts of child predators. As one security expert observed, "people who prey on children—now have the ability to get basic information about them—where they live, what they look like," cautioning that "this lapse of security" would potentially allow such predators to gain the trust of children whose information was compromised. Other security experts have expressed similar concerns: "When [the data] includes their parents as well—along with their home address—and you can link the two and emphatically say 'Here is 9 year old Mary, I know where she lives and I have other personally identifiable information about her parents (including their password and security question),' I start to run out of superlatives to even describe how bad that is."

71. In interviews since news of the Data Breach surfaced, parents have expressed dismay and outrage that their PII and that of their children was compromised. One parent said that she "was surprised and shocked to see my data breached on a 'child friendly' website," while another asked "[i]f you can't trust a company like that, then who can you trust with your information?" Likewise, a parent asked of VTech "Why do you need [to] know my address, why

do you need to know all this information just so I can download a couple of free books for my kid on this silly pad thing? Why did they have all this information?"

72. Although the hacker who has claimed responsibility for the Data Breach has said that "nothing" will be done with the compromised data, security expert Troy Hunt cautioned: "I wouldn't trust him." The data is potentially worth millions of dollars, giving the hacker and anyone else with whom the hacker shared the data strong incentives to sell it in underground markets. In this regard, the hacker might want to publicize the Data Breach and falsely make it appear that nothing would be done with the data. Or, the hacker's financial circumstances might change, leading the hacker to sell the compromised data out of necessity. Further, the hacker has made no representation that the compromised data will be destroyed or kept secure, and the hacker has shared this information with one news organization, which in turn has shared it with a security expert. Particularly in light of the hacker's illegal activities and lack of accountability, there is no reason to trust the hacker's claim that "nothing" will be done with the compromised data, and every reason for affected parents and children to proceed as though their PII has been or will be distributed or sold for nefarious purposes.

73. Moreover, given VTech's rampant security deficiencies, as well as its failure to detect the Data Breach at issue here, it is possible if not likely that other unauthorized individuals have accessed and downloaded the sensitive PII of parents and children from VTech's servers.

74. As a result of the Data Breach, Plaintiff and other VTech Customers, will have to remain vigilant for years, and possibly the rest of their lives, to combat further use of their sensitive PII by cyber criminals and child predators. Despite all of the best efforts of Plaintiff, other VTech Customers, or anyone else, the compromised sensitive PII of VTech Customers can never be made private again. Because the sensitive PII compromised in the Data Breach is

sufficient to open fraudulent accounts and difficult to change, VTech Customers' financial statements, medical bills, insurance records, utility bills, and credit reports need to be monitored to prevent unauthorized use of their compromised sensitive PII by thieves for years, and potentially for their lifetimes, and VTech Customers may reasonably expend time and money for prophylactic measures to alleviate their anxiety, stress and emotional distress, such as placing credit alerts and freezes and subscribing to credit monitoring services. Similarly, because the sensitive PII compromised in the Data Breach places Plaintiff and other VTech Customers at increased risk of exposure to criminal acts of child predators, VTech Customers may reasonably expend time and money for prophylactic measures to alleviate their anxiety, stress and emotional distress, such as educating themselves on how to protect themselves from such criminals.

75. Plaintiff and VTech Customers have also been harmed by the loss of use of VTech's online services during the time that these services are offline.

76. On November 30, VTech announced that it had suspended Learning Lodge and a number of its websites, including www.planetvtech.com, www.lumibeauxreves.com, www.pvsmilelink.com, and www.sleepybearlullabytime.com, "for thorough security assessment and fortification."

77. Similarly, in its FAQ about Data Breach on VTech Learning Lodge, updated on December 3, 2015, VTech announced that it had suspended the Kid Connect network.

78. These online services represent part of the value that customers reasonably expected when purchasing VTech devices, and customers paid a premium for products with access to these services. Further, some of the features of the VTech devices, including the features of the Kid Connect service, require these online services to function. As a result, VTech

Customers have been harmed by the loss of use of these services while they are offline and have similarly been harmed by the loss of use of their VTech devices that depend on these services.

VI. SENSITIVE PII WAS COMPROMISED AS A RESULT OF THE DATA BREACH CAUSING PLAINTIFF AND PLAINTIFF'S MINOR CHILD PRESENT INJURY AND INCREASING THEIR RISK OF FUTURE INJURY

79. Plaintiff Fredy Giron purchased a VTech Kidizoom Smartwatch DX ("VTech Device") from VTech on October 17, 2015 and signed up for Learning Lodge shortly thereafter for use by Plaintiff's minor child, because VTech represented that VTech Devices were kid-friendly and offered robust parental controls, and Plaintiff willingly paid a premium over competing products for these capabilities.

80. Plaintiff was required to sign up for Learning Lodge to allow Plaintiff's child to take full advantage of the VTech Device. In doing so, VTech required Plaintiff to provide it with sensitive PII pertaining to Plaintiff, including his name, email address, password, secret question and answer, home address, as well as his credit card number and billing information. In addition, VTech required sensitive PII about Plaintiff's minor child to be provided, including his child's name, gender, birthday, and a photograph.

81. Plaintiff provided the PII required by VTech, expecting that it would be reasonably safeguarded to maintain its confidentiality.

82. Plaintiff and Plaintiff's child regularly used the capabilities of the VTech Device offered through VTech's Learning Lodge online service.

83. To date, VTech has not notified Plaintiff of the Data Breach.

84. Plaintiff learned of the Data Breach in December 2015.

85. Due to the silence of VTech, Plaintiff spent numerous hours attempting to confirm whether the sensitive PII that Plaintiff was required to provide to VTech, so that Plaintiff's child could take full advantage of the VTech Device, had been compromised.

86. Based upon the information that Plaintiff has gathered about the Data Breach, Plaintiff has a good faith basis to believe that the sensitive PII that Plaintiff was required to provide to VTech was compromised in the Data Breach.

87. Plaintiff has continued to spend time and money, including out-of-pocket expenses, associated with the prevention, detection, and recovery from identity theft. There are also lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity data misuse.

88. If VTech had promptly notified Plaintiff that his sensitive PII had been compromised in the Data Breach, Plaintiff would have been able to expedite these steps and alleviate the anxiety, stress and emotional distress that Plaintiff has suffered as a result of Plaintiff's efforts to investigate the Data Breach and contain its impact on the compromised sensitive PII that he was required to provide to VTech.

89. Going forward, Plaintiff anticipates continuing to spend considerable time and money for the rest of Plaintiff's life to contain the impact of the Data Breach on the sensitive PII that Plaintiff was required to provide to VTech, including research and monitoring to prevent, detect, contest, and recover from identity data misuse.

90. In addition, Plaintiff and Plaintiff's minor child's regular use of VTech's Learning Lodge service was disrupted when VTech took this service offline, and this usage has not been restored to date.

VII. CLASS ACTION ALLEGATIONS

91. Plaintiff brings claims pursuant to Federal Rule of Civil Procedure 23 on behalf of a class and a subclass of similarly situated persons, which they initially propose be defined as follows:

> **Class:** All current and former parents, legal guardians, and minor children whose PII was compromised as a result of the data breach publicized in November 2015 ("VTech Customers") and whose VTech Learning Lodge and/or Kid Connect account is linked to a home address in the United States.
>
> **Overcharge Subclass:** All Class members who purchased (i) a VTech Device that connects to Learning Lodge and/or Kid Connect and/or (ii) products or services from Learning Lodge and/or Kid Connect

92. **Numerosity.** The proposed Class and Overcharge Subclass are sufficiently numerous, as millions of VTech Customers in the United States have had their PII compromised, these VTech Customers are dispersed throughout the United States making joinder of all members impracticable, and Class and Overcharge Subclass members can be readily identified by records maintained by VTech.

93. **Commonality.** Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual class members.

a. Whether VTech had a legal duty to use reasonable security measures to protect Class members' PII;

b. Whether VTech timely, accurately, and adequately informed Class members that their PII had been compromised;

c. Whether VTech breached its legal duty by failing to protect Class members' PII;

d. Whether VTech acted reasonably in securing Class members' PII;

e. Whether Class members are entitled to actual damages and/or statutory damages; and

f. Whether Class members are entitled to injunctive relief.

94. **Typicality.** Plaintiff's claims are typical of the claims of members of the proposed Class and Overcharge Subclass because, among other things, Plaintiff and Class and Overcharge Subclass members sustained similar injuries as a result of VTech's uniform wrongful conduct, and their legal claims all arise from the same conduct by VTech.

95. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the proposed Class and Overcharge Subclass. Plaintiff's interests do not conflict with Class and Overcharge Subclass members' interests, and Plaintiff has retained counsel experienced in complex class action and data privacy litigation to prosecute this case on behalf of the Class and Overcharge Subclass.

96. **Rule 23(b)(3).** In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual class members, and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing VTech's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

97. **Rule 23(b)(2).** Plaintiff also satisfies the requirements for maintaining a class action under Rule 23(b)(2). VTech has acted or refused to act on grounds that apply generally to the proposed Class and Overcharge Subclass, making final declaratory or injunctive relief appropriate with respect to the proposed Class and Overcharge Subclass as a whole.

98. **Rule 23(c)(4).** Plaintiff also satisfies the requirements for maintaining a class action under Rule 23(c)(4). The claims are composed of particular issues that are common to all Class members and capable of class-wide resolution that will significantly advance the litigation.

VIII. CAUSES OF ACTION

COUNT I: Negligence

99. Plaintiff realleges and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

100. Plaintiff alleges this count on behalf of the Class.

101. In collecting and retaining the sensitive PII of VTech Customers, VTech, as a manufacturer of internet-enabled devices for children, owed Plaintiff and Class members a duty to exercise reasonable safeguarding and protecting that information. This duty included, among other things, maintaining and testing VTech's security systems and taking other reasonable security measures to protect and adequately secure the PII of Plaintiff and Class members from unauthorized access.

102. VTech's security system and procedures for handling the sensitive PII of Class members were intended to and did affect Plaintiff and Class members. VTech knew that by collecting and storing the sensitive PII of VTech Customers, it undertook a responsibility to take reasonable security measures to protect the information from being stolen and exposed to unauthorized persons.

103. VTech owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate security practices. It was foreseeable that if VTech did not take reasonable security measures, Plaintiff's and Class members' PII would be stolen. VTech knew or should have known its security systems were inadequate, but VTech failed to take reasonable precautions to safeguard Plaintiff's and Class members' PII.

104. The duty VTech owed to Plaintiff and Class members to protect their PII is underscored by the Illinois Personal Information Protection Act, Ill. Comp. Stat. Ann. 530/10(a), *et seq.*, which recognizes the importance of maintaining the confidentiality of PII, and which was enacted to protect individuals from the unauthorized exposure of their PII, as well as the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, *et seq.*("COPPA") and its associated regulations at 16 C.F.R. §312.1, *et seq.*, which restricts "the collection, use, and/or disclosure of personal information from and about children on the Internet."

105. VTech also had a duty to timely disclose to Plaintiff and Class members that their PII had been or was reasonably believed to have been compromised. Timely disclosure was necessary so that Plaintiff and Class members could take prophylactic measures to necessary to alleviate anxiety, stress and emotional distress associated with protecting themselves from identity thieves, fraud, and child predators, including among other things: (i) buying identity protection, monitoring, and recovery services; (ii) flagging asset, credit, and tax accounts for fraud; (iii) purchasing or otherwise obtaining credit reports; (iv) monitoring credit, financial, utility, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, and charges; (v) placing and renewing credit fraud alerts on a quarterly basis; (vi) routinely monitoring public records, loan data, or criminal records; (vii) contesting fraudulent charges and other forms of criminal and financial identity theft, and repairing damage to credit and other financial accounts; and (viii) taking other steps to protect themselves from identity theft, fraud, and child predators, which requires the expenditure of time, effort and/or money.

106. VTech has admitted that Class member PII was exposed as a result of the Data Breach. As a result of VTech's negligence, Plaintiff and members of the Class have suffered and

will suffer injury, including but not necessarily limited to: (1) anxiety, stress and emotional distress; (2) the loss of the opportunity to control how their PII is used; (3) the diminution in the value and/or use of PII entrusted to VTech for the purpose of deriving services from VTech, when Plaintiff and Class members understood that their sensitive PII would be safeguarded against theft and misuse by others; (4) the compromise, publication, and/or theft of their sensitive PII; (5) out-of-pocket costs associated with prophylactic measures taken to prevent, detect, and recover from identity theft; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from sensitive PII misuse; (6) costs associated with the ability to use credit and assets frozen or flagged for fraud, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial and/or health care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, which remains in VTech's possession and is subject to further breaches so long as VTech fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for years, and possibly the remainder of the Class members' lives.

107. There is a very close connection between VTech's failure to use reasonable security protections of Class member PII and the injuries suffered by Plaintiff and Class members. Class members have had their sensitive PII compromised, face a resulting increased

risk of financial, physical, and/or emotional harm from criminals and child predators, and need to act to prevent being further victimized as a result of further unauthorized access to their sensitive PII—or to recover from such further victimization—by taking prophylactic and/or mitigating measures, which may include: (i) buying identity protection, monitoring, and recovery services; (ii) freezing or flagging asset, credit, and tax accounts for fraud; (iii) purchasing or otherwise obtain credit reports; (iv) monitoring credit, financial, utility, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, and/or charges; (v) placing and renewing credit fraud alerts on a quarterly basis; (vi) routinely monitoring public records, loan data, and criminal records; (vii) contesting fraudulent charges and other forms of criminal and financial identity theft, and repair damage to credit and other financial accounts; and (viii) taking other steps to protect themselves and recover from identity theft, fraud and child predators.

108. VTech is responsible for not protecting the PII of the Class members. If VTech had reasonable security measures in place, cyber thieves would not have been able to steal and expose Class members' PII.

109. The policy of preventing future harm weighs strongly in favor of finding a special relationship between VTech and Class members. VTech was entrusted with Plaintiff and Class members' sensitive personal information as a condition for obtaining full use of goods and services from VTech, and Plaintiff and Class members depended on VTech to ensure that this information was protected from theft and unauthorized disclosure. If VTech is not held accountable for failing to take reasonable security measures to protect non-financial, but sensitive, customer PII of parents, legal guardians, and minor children, it will not take the steps that are necessary to protect against future data breaches.

110. VTech breached its duty to exercise reasonable care in protecting the PII of Plaintiff and the Class by failing to implement and maintain adequate security measures to safeguard PII, failing to monitor its systems to identify suspicious activity, and allowing unauthorized access to the PII of Plaintiff and Class members.

111. VTech breached its duty to detect and timely notify Plaintiff and the Class about the Data Breach.

112. But for VTech's failure to implement and maintain adequate security measures to protect Class members' PII and failure to monitor its systems to identify suspicious activity, the PII of Plaintiff and Class members would not have been stolen, Plaintiff and Class members would not have been injured, and Plaintiff and Class members would not be at a heightened risk of identity theft in the future.

113. VTech's negligence was a substantial factor in causing harm to Plaintiff and Class members. As a direct and proximate result of VTech's failure to exercise reasonable care and use commercially reasonable security measures, Plaintiff's and Class members' PII was accessed by unauthorized individuals, who can allow this compromised PII to be used by thieves and child predators to financially, physically, and/or emotionally injure Plaintiff and Class members.

114. As a result of VTech's negligence, Plaintiff and members of the Class are entitled to injunctive relief, including, but not limited to an order that VTech: (1) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on VTech's systems on a periodic basis; (2) engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) audit, test, and train its security personnel regarding any new or modified

procedures; (4) purge, delete and destroy, in a secure manner, Class member PII not necessary for its business operations; (5) conduct regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receive periodic compliance audits by a third party regarding the security of the computer systems VTech uses to store the personal information of customers; (8) meaningfully educate Plaintiff and Class members about the financial, physical, and emotional threats they face from thieves and child predators as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves; and (9) provide ongoing identity theft protection, monitoring, and recovery services to Plaintiff, and Class members.

115. Plaintiff and the Class are also entitled to damages and reasonable attorneys' fees and costs. Plaintiff also seeks reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23.

COUNT II: Declaratory Judgment

116. Plaintiff realleges and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

117. Plaintiff alleges this count on behalf of the Class.

118. As previously alleged, Plaintiff and the Class have stated claims against VTech based on negligence.

119. VTech has failed to live up to its obligations to provide reasonable security measures for the PII of Plaintiff and the Class, as indicated by the Data Breach that precipitated this lawsuit.

120. In addition, the Data Breach has rendered VTech's system even more vulnerable to unauthorized access and requires that VTech immediately take even more stringent measures to currently safeguard the PII of Plaintiff and the Class going forward.

121. An actual controversy has arisen in the wake of VTech's Data Breach regarding VTech's *current* obligations to provide reasonable data security measures to protect the non-financial PII of Plaintiff and the Class. While VTech has taken Learning Lodge and Kid Connect offline due to admittedly inadequate data security, VTech has not specified how it intends to satisfy its current obligation to better safeguard the non-financial PII of Plaintiff and the Class.

122. Plaintiff thus seeks a declaration that, to comply with its existing obligations, VTech must implement specific additional, prudent industry security practices, as outlined below, to provide reasonable protection and security to the non-financial PII of Plaintiff and the Class.

123. Specifically, Plaintiff and the Class seek a declaration that (a) VTech's existing security measures do not comply with its obligations, and (b) that to comply with its obligations, VTech must implement and maintain reasonable security measures on behalf of Plaintiff and the Class, including, but not limited to: (1) engaging third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on VTech's systems on a periodic basis; (2) engaging third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) auditing, testing, and training its security personnel regarding any new or modified procedures; (4) purging, deleting and destroying, in a secure manner, customer data not necessary for its business operations; (5) conducting regular database scanning and securing checks consistent with prudent industry

practices; (6) periodically conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receiving periodic compliance audits by a third party regarding the security of the computer systems VTech uses to store the personal information of customers; (8) meaningfully educating Plaintiff and Class members about the financial, physical, and emotional threats they face from thieves and child predators as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves; and (9) providing ongoing identity theft protection, monitoring, and recovery services to Plaintiff, and Class members.

COUNT III: Breach of Contract

124. Plaintiff realleges and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

125. Plaintiff brings this count on behalf of the Class and the Overcharge Subclass.

126. The internet-capable features of the VTech Devices could not be used without creating a digital accounts with VTech to access these features on Learning Lodge and/or Kid Connect.

127. Plaintiff and the Overcharge Subclass Members purchased VTech Devices, expecting that trusted adults and children would be able to use these features of the VTech Devices.

128. When Plaintiff and Class Members created the required digital account with VTech to access these features, they were required to indicate that they read and agreed to VTech's Terms and Conditions and Privacy Statement, which included security protections for their sensitive PII.

129. As a result of VTech's Terms and Conditions and Privacy Statement, VTech was obliged to implement adequate security protocols to protect the sensitive PII of Plaintiff and Class members.

130. Plaintiff and Class members and Overcharge Subclass members performed their obligations under the contract because, among other things, Subclass members paid the purchase price for (i) VTech Devices that connect to Learning Lodge or Kid Connect and/or (ii) apps, games, e-books, or other content from Learning Lodge or Kid Connect, and Class members abided by the Terms and Conditions and Privacy Statement.

131. The Data Breach, however, revealed that VTech breached the material term of its contract with Plaintiff and Class members to protect the sensitive PII of Plaintiff and Class members.

132. Consumers of internet-capable electronic products for children, including Plaintiff and Class members, value the ability to control data that their children access as well as data that is accessed about them. Children's products and children's online services that do not use industry standard data security protocols to protect customer sensitive PII are fundamentally less useful and valuable to customers such as Plaintiff, Class members, and Overcharge Subclass members than children's products and children's online services that use industry standard security protections. Consumers, including Plaintiff, Class members, and Overcharge Subclass members, will, if given the choice between two otherwise identical products and services, purchase and use the ones with industry-standard security practices over ones with substandard security practices (to the extent ones that use substandard security protocols can sell their products and services at all).

133. Plaintiff and Class members had a reasonable expectation that they would receive adequate protection for the sensitive PII of Plaintiff and Class members as part of the purchase price for products and services from VTech, and those security protections were valuable to Plaintiff, Class members, and Overcharge Subclass members.

134. To Plaintiff, Class members, and Overcharge Subclass members, the as-promised products and services offer significantly more utility than the products and services delivered, which lacked meaningful security protections.

135. Thus, to Plaintiff and the Overcharge Subclass members, the products and services promised and paid-for were substantially more valuable than the unsecure products and services delivered.

136. Plaintiff and Overcharge Subclass members paid for, but never received, the valuable security protections to which they were entitled, and which would have made their VTech products and services significantly more useful to the Class members.

137. As a result of VTech's misconduct and breach of contract described herein, Plaintiff and the Class members suffered and will continue to suffer injury and/or harm including, but not limited to, anxiety, stress, emotional distress, loss of privacy, and other economic and non-economic losses. Looking forward, and recognizing the risk caused by devastating data breaches like VTech's, Plaintiff and Class members will have to incur expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; and increased risk of future harm.

138. In addition, Plaintiff and Overcharge Subclass members suffered actual damages, including an amount equal to the difference in the free-market value of the secure products and services they paid for and the insecure products and services they received.

139. Accordingly, Plaintiff, on behalf of himself and Class members and Subclass members, seeks an order declaring that VTech's conduct constitutes breach of contract, and awarding Plaintiff and Class and Subclass members damages as described above.

COUNT IV: Breach of Covenant of Good Faith and Fair Dealing

140. Plaintiff realleges and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

141. Plaintiff brings this count on behalf of the Class and the Overcharge Subclass.

142. Plaintiff and Class members formed a contract with Defendant that contained an implied covenant of good faith and fair dealing, which obligated Defendant to provide reasonable and adequate safeguards for the PII it collected from Plaintiff and Class members.

143. Defendant breached this implied covenant of good faith and fair dealing by failing to provide reasonable and adequate safeguards for the PII it collected from Plaintiff and Class members.

144. As a direct and proximate result of this breach, Plaintiff and Class members suffered and will continue to suffer injury and/or harm including, but not limited to, anxiety, stress, emotional distress, loss of privacy, and other economic and non-economic losses. Looking forward, and recognizing the risk caused by devastating data breaches like VTech's, Plaintiff and Class members will have to incur expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; and increased risk of future harm.

145. In addition, Plaintiff and Overcharge Subclass members suffered actual damages, including an amount equal to the difference in the free-market value of the secure products and services they paid for and the insecure products and services they received.

146. Accordingly, Plaintiff, on behalf of himself and Class members and Subclass members, seeks an order declaring that VTech's conduct constitutes breach of the covenant of good faith and fair dealing, and awarding Plaintiff and Class and Subclass members damages as described above.

COUNT V: Implied Warranty of Merchantability

147. Plaintiff realleges and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

148. Plaintiff brings this count on behalf of the Class and the Overcharge Subclass.

149. Defendant is and was at all relevant times a manufacturer and merchant with respect to the VTech Devices at issue that were purchased by Plaintiff and Class members.

150. The VTech Devices purchased by Plaintiff and Class Members included access to VTech's online services Learning Lodge and/or Kid Connect.

151. Plaintiff and Class members formed a contract with Defendant that contained an implied warranties of merchantability, which obligated and imposed a duty upon Defendant that its devices and online services be fit for the ordinary purposes for which they are used and conform to the promises or affirmations of fact made on the container or label.

152. Defendant has not validly or effectively disclaimed, excluded, or modified these implied warranties of merchantability.

153. Plaintiff and Class members have used the VTech Devices and online services that they purchased in a manner consistent with their intended use.

154. Defendant breached this implied warranty of merchantability, in that its devices and online services were not fit for the ordinary purposes for which they are to be used, nor do they conform to the promises or affirmations of fact made on the container or label, because Defendant failed to provide reasonable and adequate safeguards for the PII it collected from Plaintiff and Class members, and its devices are unable to access the Learning Lodge and/or Kid Connect online services.

155. As a direct and proximate result of this breach, Plaintiff and the Class members suffered and will continue to suffer injury and/or harm including, but not limited to, anxiety, stress, emotional distress, loss of privacy, and other economic and non-economic losses. Looking forward, and recognizing the risk caused by devastating data breaches like VTech's, Plaintiff and Class members will have to incur expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; and increased risk of future harm.

156. In addition, Plaintiff and Overcharge Subclass members suffered actual damages, including an amount equal to the difference in the free-market value of the secure products and services they paid for and the insecure products and services they received.

157. Accordingly, Plaintiff, on behalf of himself and Class members and Subclass members, seeks an order declaring that VTech's conduct constitutes breach of the implied warranty of merchantability, and awarding Plaintiff and Class and Subclass members damages as described above.

COUNT VI: Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act 815 ILCS §§ 505/1, *et seq.*

158. Plaintiff realleges and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

159. Plaintiff brings this count on behalf of the Overcharge Subclass.

160. The Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA") (815 ILCS §§ 505/1, et seq.) protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

161. The ICFA prohibits any unlawful, unfair, or fraudulent business acts or practices including the employment of any deception, fraud, false pretense, false promise, false advertising, misrepresentation, or the concealment, suppression, or omission of any material fact.

162. The ICFA applies to Defendant's actions and conduct as described herein because it protects consumers in transactions that are intended to result, or which have resulted, in the sale of goods or services.

163. Defendant is a "person" as defined under section 505/1(c) of the ICFA.

164. Plaintiff and each Overcharge Subclass member is a "consumer" as defined under section 505/1(e) of the ICFA.

165. Defendant's VTech Devices that connect to Learning Lodge and/or Kid Connect and apps, games, e-books, or other content from Learning Lodge and/or Kid Connect are "merchandise" within the meaning of section 505/1(b) and their sale is considered "trade" or "commerce" under the ICFA.

166. Defendant violated the ICFA by misrepresenting and/or omitting material facts about its VTech Devices and content from Learning Lodge and/or Kid Connect.

167. Defendant represented that its products and database would keep information that it required Plaintiff and each Overcharge Subclass member to provide secure, when, in fact, it failed to use even the most basic security measures available to keep information safe.

168. Despite Defendant's representations, its products and services did not live up to the level of US safety standards. It is well-recognized that services that use the Internet to transmit and store information in databases should be protected from SQL injection attacks, and in fact can be protected from such attacks via certain defenses and protocols—either in the network, or in the applications, themselves.

169. Specifically, Defendant failed to disclose that it was:

- Storing passwords as simple, "unsalted," hashes;
- Storing secret questions for password and account recovery in plaintext;
- Linking children's accounts to home address and other identifying information;
- Failing to use encryption for the transmission of collected data (i.e., no SSL);
- Failing to encrypted stored data;
- Failing to protect against SQL injection;
- Storing customer data in an Internet-accessible database;
- Sharing and transmitting collected customer data with an unauthorized party; and
- Failing to implement basic user authentication (e.g., by limiting who can gain "root" access).

170. Defendant was aware or should have been aware that it was not implementing security protections as outlined above.

171. Defendant misrepresented and/or omitted the material fact that its VTech Devices and content from Learning Lodge and/or Kid Connect do not offer adequate security protections in both their advertising and warnings on the VTech Devices' physical packaging.

172. Defendant knew and was aware that if it prominently disclosed on the VTech Devices' physical packaging that it does not offer any data security protections, it would have to sell the VTech Devices at a substantially lower price.

173. Defendant created its advertisements and marketing materials with the intent that Plaintiff and Overcharge Subclass members would rely on the information provided, but omitted the material fact that the VTech Devices do not offer adequate security protections.

174. Had Defendant not engaged in the misrepresentations and/or deceptive omission of material facts described above, Plaintiff and the Overcharge Subclass members would have been presented with an informed choice as to whether or not to buy the VTech Devices and would have also been presented with the disclosures necessary to modify their use of (and their children's use of) the VTech Devices to avoid a breach of their privacy.

175. Defendant's material misrepresentations and omissions to Plaintiff and the Overcharge Subclass members constitute unfair and deceptive acts or practices in violation of the ICFA. Plaintiff and reasonable Overcharge Subclass members would not have purchased the VTech Devices if the Defendant disclosed that it was not secure.

176. Plaintiff and the Overcharge Subclass members were damaged by Defendant's conduct directed towards consumers. Defendant misrepresented the safety of its products and database and chose not to disclose that its VTech Devices were not secure, because Defendant wanted to create demand for and to sell the VTech Devices. Had Defendant disclosed its true security practices, Plaintiff and the Class members either would have not purchased the VTech

Devices or would have paid substantially less for them (i.e., the value of VTech Devices without adequate security protections is worth substantially less than the value of similar devices with adequate protection).

177. As a direct and proximate result of Defendant's violation of the ICFA, Plaintiff and the each Overcharge Subclass member have suffered harm in the form of monies paid for Defendant's products. Plaintiff, on behalf of himself and the Class, seeks an order (1) requiring Defendant to cease the unfair practices described herein; (2) awarding damages, interest, and reasonable attorneys' fees, expenses, and costs to the extent allowable; and/or (3) requiring Defendant to restore to Plaintiff and each Overcharge Subclass member any money acquired by means of unfair competition (restitution).

COUNT VII: Unjust Enrichment

178. Plaintiff realleges and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

179. Plaintiff brings this count in the alternative on behalf of the Overcharge Subclass.

180. Plaintiff and the Overcharge Subclass conferred a monetary benefit on VTech in the form of monies paid for the purchase of goods and services from VTech.

181. VTech appreciates or has knowledge of the benefits conferred directly upon it by Plaintiff and the Overcharge Subclass.

182. The monies paid for the purchase of goods and services by Plaintiff and the Overcharge Subclass to VTech were supposed to be used by VTech, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and the Class.

183. VTech failed to provide reasonable security, safeguards and protection to the PII of Plaintiff and the Class, and, as a result, Plaintiff and members of the Overcharge Subclass overpaid VTech for the goods and services purchased from VTech.

184. Under principles of equity and good conscience, VTech should not be permitted to retain the money belonging to Plaintiff and members of the Overcharge Subclass, because VTech failed to provide adequate safeguards and security measures to protect the PII of Plaintiff and the Class that the Overcharge Subclass paid for but Plaintiff and the Class did not receive.

185. As a result of VTech's conduct as set forth in this Complaint, Plaintiff and the Overcharge Subclass suffered damages and losses as stated above, including monies paid for VTech products and services that Plaintiff and the Overcharge Subclass members would not have purchased had VTech disclosed the materials facts that it lacked adequate measures to safeguard customers' data and had VTech provided timely and accurate notice of the data breach, and including the difference between the price they paid for VTech's products and services as promised and the actual diminished value of its goods and services.

186. Plaintiff and Overcharge Subclass members have conferred directly upon VTech an economic benefit in the nature of monies received and profits resulting from sales and unlawful overcharges to the economic detriment of Plaintiff and the Overcharge Subclass.

187. The economic benefit, including the monies paid and the overcharges and profits derived by VTech and paid by Plaintiff and Overcharge Class Members, is a direct and proximate result of VTech's unlawful practices as set forth in this Complaint.

188. The financial benefits derived by VTech rightfully belong to Plaintiff and the Class members.

189. It would be inequitable under established unjust enrichment principles in the District of Columbia and all of the 50 states for VTech to be permitted to retain any of the financial benefits, monies, profits and overcharges derived from VTech's unlawful conduct as set forth in this Complaint.

190. VTech should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Overcharge Subclass all unlawful or inequitable proceeds received by VTech.

191. A constructive trust should be imposed upon all unlawful or inequitable sums received by VTech traceable to Plaintiff and the Overcharge Subclass.

192. Plaintiff and the Overcharge Subclass have no adequate remedy at law.

IX. PRAYER FOR RELIEF

Plaintiff, on behalf of himself and on behalf of the proposed Class and Overcharge Subclass, requests that the Court:

a. Certify this case as a class action, appoint Plaintiff as Class and Overcharge Subclass representative, and appoint Plaintiff's counsel to represent the Class and Overcharge Subclass;

b. Find that VTech breached its duty to safeguard and protect the PII of Plaintiff and the Class members that was compromised in the Data Breach;

c. Award Plaintiff and Class and Overcharge Subclass members appropriate relief, including actual and statutory damages, restitution and disgorgement;

d. Award equitable, injunctive and declaratory relief as may be appropriate;

e. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

f. Award pre-judgment and post-judgment interest as prescribed by law; and

g. Grant additional legal or equitable relief as this Court may find just and proper.

X. JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: December 31, 2015

Respectfully submitted,

By: /s/ Ryan F. Stephan

Ryan F. Stephan
James B. Zouras
Andrew C. Ficzko
RStephan@stephanzouras.com
Jzouras@stephanzouras.com
Aficzko@stephanzouras.com
STEPHAN ZOURAS, LLP
205 North Michigan Avenue
Suite 2560
Chicago, Illinois 60601
Telephone: (312) 233-1550
Facsimile: (312) 233-1560

Cari Campen Laufenberg, *Pro hac vice forthcoming*
claufenberg@kellerrohrback.com
Gretchen Freeman Cappio, *Pro hac vice forthcoming*
gcappio@kellerrohrback.com
Amy N. L. Hanson, *Pro hac vice forthcoming*
ahanson@kellerrohrback.com
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Telephone: (206) 623-1900
Facsimile: (206) 623-3384

Counsel for the Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on December 31, 2015, a true and correct copy of the foregoing **COMPLAINT** was filed via this Court's CM/ECF system.

s/ Ryan F. Stephan
Ryan F. Stephan